EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond

Karl Koscher
University of Washington

Ari Juels
RSA Labs

Tadayoshi Kohno
University of Washington

Vjekoslav Brajkovic
University of Washington

ABSTRACT

EPC (Electronic Product Code) tags are industry-standard RFID devices poised to supplant optical barcodes in many applications. They are prevalent in case and pallet tracking, and also percolating into individual consumer items and border-crossing documents.

In this paper, we explore the systemic risks and challenges created by increasingly common use of EPC for security applications. As a central case study, we examine the recently issued United States Passport Card and Washington State "enhanced" drivers license (WA EDL), both of which incorporate Gen-2 EPC tags. We explore several issues:

1. **Cloning:** We report on the data format of Passport Cards and WA EDLs and demonstrate their apparent susceptibility to straightforward cloning into off-the-shelf EPC tags. We show that a key anti-cloning feature proposed by the U.S. Department of Homeland Security (the tag-unique TID) remains undeployed in these cards.

2. **Read ranges:** We detail experiments on the read-range of Passport Cards and WA EDLs across a variety of physical configurations. These read ranges help characterize both issues regarding owner privacy and vulnerability to clandestine "skimming" and cloning.

3. **Design drift:** We find that unlike Passport Cards, WA EDLs are vulnerable to scanning while placed in protective sleeves, and also to denial-of-service attacks and covert-channel attacks.

We consider the implications of these vulnerabilities to overall system security, and offer suggestions for improvement. We also demonstrate anti-cloning techniques for off-the-shelf EPC tags, overcoming practical challenges in a previous proposal to co-opt the EPC "kill" command to achieve tag authentication.

Our aim in this paper is to fill a vacuum of experimentally grounded guidance on security applications for EPC tags not just in identity documents, but more broadly in the authentication of objects and people.

Key words: authentication, cloning, EPC, PASS, passport card, RFID, WHTI.

1. INTRODUCTION

EPC (Electronic Product Code) tags [19] are RFID devices poised to supplant optical barcodes in a wide variety of applications. Today EPC tags figure most prominently in the tracking of cases and pallets in supply chains. Proponents of the technology envision a future in which tagging of individual items facilitates a full life-cycle of automation from shop floors to retail points of sale, in home appliances, and through to recycling facilities.

As one example of this application, EPC tags are seeing a landmark deployment this year in the U.S. in identity documents used at national border crossings. The United States Passport Card (also known as the PASS Card), a land-border and seaport entry document first issued in the summer of 2008, incorporates an EPC tag. This identity document was issued in response to the Western Hemisphere Travel Initiative (WHTI) [46], which, among others, phases out exemptions in document requirements for border crossing (previously, United States and Canadian citizens only had to present photo ID and a birth certificate). Certain states have issued or plan to issue Enhanced Drivers Licenses (EDLs), WHTI-compliant documents, which will also make use of EPC. Washington State started issuing EDLs in early 2008 [32], with New York State following in September 2008 [2].

To date, the only form of EPC ratified as a technical standard by EPCglobal, the body that oversees EPC development, is the Class-1 Gen-2 tag. (For brevity, we refer to this tag simply as a "Gen-2" or "EPC" tag in this paper.) Passport Cards and other WHTI documents will incorporate this type of EPC tag, and it is likely to see the greatest use in barcode-type RFID applications as well for some time to come. EPC tags are attractive for their low cost (below ten U.S. cents each). Also, thanks to their operation in the Ultra-High Frequency (UHF) spectrum (860–960 Mhz), they have a relatively long read range—tens of feet under benign conditions [39].

Gen-2 tags, however, are essentially wireless barcodes, with no specific provisions to meet security and privacy needs. Just as their optical counterparts are subject to photocopying, Gen-2 EPC tags are vulnerable to *cloning attacks* in which their publicly visible data are scanned ("skimmed") by an adversary and then transferred to a clone device—be it another tag or a more sophisticated emulator.

1.1 Our contribution: vulnerability analysis

In this paper, we consider the use of EPC tags in security applications. We emphasize a systemic approach, examining

low-level security features and discussing their significance in potential real-world deployment scenarios. We realize that not all of these attacks will be applicable all the time in the U.S. border crossing scenarios, but we feel that they may be applicable at some times if appropriate procedures are not in place, or may be applicable to other countries wishing to deploy similar technologies. We focus on Passport Cards and EDLs as an important case study in the use of EPC for security applications, and an early example of EPC deployment with unequivocal security requirements.

In its final rule on the Passport Card [3], the Department of State acknowledged a range of objections expressed in responses to its proposed rule of 2006 [4]; four Members of Congress expressed concerns about the security and privacy of the Passport Card. The Department indicated that many commenters did not understand "the business model that WHTI is designed to meet," and cited a need for simultaneous reading of multiple EPC tags as a motivation for its choice of EPC ("vicinity read RFID") as well as the technology's amenability to passenger pre-processing, i.e., its relatively long read range. ("Proximity-read" RFID devices, i.e., contactless smartcards, do not have these benefits, and some other classes of RFIDs only have the former benefit but not the latter.) The Department additionally noted that on May 1, 2007, the National Institute for Standards and Technology (NIST) certified the Passport Card as, "meeting or exceeding ISO security standards... and the best available practices for protection of personal identification documents." Finally, the Department observed that Passport Cards will not carry personally identifiable information, and will be issued with protective sleeves, radio-opaque envelopes that help prevent unwanted scanning.

We have obtained a Passport Card and two Washington State EDLs for our experiments. We show first that the publicly readable data in both types of identity document can be straightforwardly cloned after a single read. Significantly, our analysis shows that Passport Cards and Washington State EDLs do not carry tag-unique, or even system-unique TIDs, but instead bear generic manufacturer codes.[1] The Tag Identifier (TID) of an EPC, a tag-specific serial number that may be factory programmed, is often held forth as an anti-cloning mechanism for EPC tags. In its Privacy Impact Assessment of the Passport Card, the U.S. Department of Homeland Security (DHS) in fact highlights tag-specific TIDs as a "powerful tool" for anti-counterfeiting [31]. As Passport Cards and Washington State EDLs do not carry specially formulated TIDs, however, their readable contents are subject to direct copying into another off-the-shelf EPC tag.

Our observations about cloning only apply to a tag's publicly readable data. Tags contain some private data in the form of PINs, which may be tag unique. Hence it is possible in principle (although improbable in our view) that a weak form of access-based authentication—an unorthodox security protocol we describe below—is in use at border crossings. In this case, reliable tag cloning would require either eavesdropping on a tag interrogation at the border or physically invasive attacks on a target identity document. Without ourselves eavesdropping on a tag interrogation at a border crossing, we are unable to determine whether or not this technique is being deployed. We note, though, that access-based authentication is not an explicitly supported feature for EPC tags. The only reference to the technique of which we are aware is a research paper [21]. Other techniques, such as detection of unique radio fingerprints [14] are also a possibility in principle, but in practice very challenging for highly constrained devices such as RFID tags.

Given the ostensible vulnerability of identity documents and other Gen-2 EPC-tagged items to cloning, a key security issue is the range at which an EPC tag is subject to clandestine reading. As owners may be expected to carry their tags in any of a variety of different circumstances, we explore read ranges within several different physical environments.

We find that both Passport Cards and EDLs are subject to reading at a distance of at least 50 meters under optimal scan conditions (down a long hallway, but still operating within FCC limits). Surprisingly, although the human body—its constituent water, in particular—is known to interfere with EPC tag reading, we find that an EDL in a wallet near the body is still subject to scanning at a distance of at least two meters. We find that the Passport Card is not readable in a well maintained protective sleeve—although it is readable under certain circumstances in a crumpled sleeve. Most surprisingly, perhaps, we find that an EDL in a protective sleeve is readable at a distance of some tens of centimeters. To the best of our knowledge, our work here in fact represents the first multifaceted characterization of EPC read ranges from the vantage point of privacy.

Our scanning experiments have a bearing not just on cloning, but also on owner privacy: While the tags do not contain personally identifiable information, they do contain unique serial numbers that can support clandestine tracking [22]. Of course, other wireless devices, like Bluetooth peripherals [20], 802.11 [15], and ANT [36], are similar in this regard, though the exposure for Passport Cards and EDLs may be greater due to their usage models.

We also find evidence that EDLs are vulnerable to denial-of-service and covert-channel attacks. These vulnerabilities stem from issuance of the cards without protection of the PIN for their tag-disablement feature, the "kill" command. Passport Cards do not have similar weaknesses. These flaws, along with EDLs' heightened susceptibility to in-sleeve scanning, would seem to point to either a form of design drift in which technical protections implemented at the federal level did not benefit Washington State in the extension to EDLs, or the risks associated with implementing a technology before the precise security requirements have been finalized.

1.2 Our contribution: countermeasures and recommendations

We emphasize that the security impact of tag vulnerabilities depends upon the operational environment. Copying of a Passport Card or EDL does not automatically ensure successful use at a border crossing. The card is linked via a back-end system to a photo of its bearer which border agents use for confirmation of traveler identities. Hence, we discuss the systemic significance of the vulnerabilities we have identified.

We argue that Passport Cards and EDLs will play a role in the border-crossing process that may give impactful prominence to the data contained in the EPC tags. Like many security processes, the passenger screening process benefits

[1] DHS claims that they learned of the existence of tag-unique TIDs too late to be incorporated into these cards, but have recommended its inclusion in future WHTI-compliant documents, including EDLs from other states.

from multiple layers of security, including physical inspection of passengers and documents. But as the EPC code can trigger a watchlist lookup, it serves as a frontline mechanism for passenger screening. As we discuss in section 5.1, the literature on cognitive biases suggests a risk that the EPC-layer of the security system will exercise undue influence over passenger screening.

We argue that even if EPC-enabled identity documents provide adequate security at border crossings, they create a system with delicate dependence on well conceived and tightly executed border crossing procedures and card issuance. Our observations on the relative weakness of EDL in comparison with Passport Cards, for example, support the idea that states may not be as well equipped to enforce good security practices around document issuance as DHS, or that there was or is not sufficient guidance from the DHS.

Given these concerns, we review the operational environment of the Passport Cards / EDLs and offer some basic procedural recommendations for the use of EPC-enabled identity documents and some technical recommendations. With this constructive motivation, we show that the elementary security features in EPC tags can be co-opted to serve as a deterrent to cloning. EPC tags include PIN-based protections both on tag disablement ("killing") and modification of tag data contents. Previous research [21] proposed techniques for co-opting these features in the service of tag *authentication*, i.e., anti-counterfeiting, but offered no experimental validation. We demonstrate that implementation of "kill" co-opting techniques is indeed feasible in deployed tags, but presents some delicate technical challenges. We explore some promising initial approaches to overcoming these challenges.

We believe that the lessons drawn from our case study in this paper will provide valuable guidance for the deployment of EPC tags in many security applications beyond border-crossing, such as anti-counterfeiting and secure item pedigrees for pharmaceutical supply chains [45].

Organization

In section 2, we briefly review related work on RFID security. We present our observations on the data format of the Washington State EDL and Passport Cards in section 3. We describe our exploration of defensive techniques in section 4. In section 5, we briefly consider the operational environment of the Passport Card / EDL and offering some procedural recommendations to prevent the use of cloned documents. We conclude in section 6 with a brief discussion of the broader implications of our findings. In the paper appendix, we provide supplementary data for our experiments, and also images of the antennas embedded in a Passport Card and EDL.

2. RELATED WORK

There have been a number of radio-layer cloning attacks against RFID tags. Westhues developed a device called the Proxmark that he successfully used to clone both proximity cards [48] as well as the VeriChip^{TM} [16], a human-implantable RFID tag. The devices targeted by Westhues emit static identifiers, i.e., they are essentially wireless barcodes. Class-1 Gen-2 EPC tags are similar in flavor to these devices, but operate in a much higher frequency band for which signal-processing is more complicated.

Bono et al. [8] reverse engineered and mounted brute-force key-cracking attacks against the Texas Instruments DST, a cryptographically enabled RFID device with short (40-bit) keys. Similarly, Nohl et al. [27] have recently reverse-engineered the Philips Mifare RFID tag and revealed structural weaknesses in its cipher and random-number generator. Heydt-Benjamin et al. [17] demonstrated cloning attacks against a set of first-generation RFID-enabled credit cards.

RFID tags saw their first prominent appearance in identity documents as additions to e-passports. Grunwald [30] cloned the chip in an RFID-enabled passport in the fullest sense, transferring the data from one chip to another. Juels, Molnar, and Wagner [23] discuss the security implications of e-passport cloning. E-passports differ from Passport Cards in that they perform cryptographic authentication. The Smart Card Alliance, among other organizations, noted the risks of EPC cloning in its response to the initial DHS WHTI proposal [5].

Some commercially available RFID tags include strong cryptography for challenge-response authentication. These tend to be relatively expensive and have constrained range. The literature is replete with techniques for implementing lower-cost cryptography in RFID tags. See, e.g., [22] for a survey and [7] for an up-to-date bibliography.

In view of the prevalence of Gen-2 EPC tags, Juels [21] proposed techniques for authenticating these tags using two existing commands, KILL and ACCESS. In section 4, we report on our implementation of these techniques and the practical challenges they pose.

3. EXPERIMENTAL EVALUATION OF PASSPORT CARD AND EDLS

3.1 Weakness in the TID-based anti-cloning mechanism

As mentioned above, EPC tags contain a data field known as the Tag Identifier (TID). At the discretion of the EPC manufacturer, this value may be factory programmed and locked, thereby ensuring that tags have permanent unique identities and (theoretically) cannot be cross-copied.

In its Privacy Impact Assessment (PIA) on the Passport Card [31], the United States Department of Homeland Security posits that:

> ...the risk of cloning RFID enabled cards and an impostor with similar physical features gaining illegal entry into the U.S., while unlikely, is real. Fortunately, there is a powerful tool that can be used to remove the risk of cloning. This tool is the Tag Identifier, or TID. The TID is available on all Gen 2 RFID tags.

However, the Gen-2 standard only requires that the TID identify the manufacturer, as well as enough additional information to determine the tag's capabilities. In particular, two classes of TIDs are defined: the $E0_h$ class, where the TID consists of a manufacturer ID and a 48-bit serial number, and the $E2_h$ class, which merely defines the manufacturer and model. The TID reported by our Passport Card is **E2 00 34 11 FF B8 00 00 00 02**, which corresponds to an $E2_h$-class Alien Higgs tag. [28] states that the bytes after the manufacturer and model IDs (starting with

FF) are Alien-specific configuration values, and using a new Higgs tag, we experimentally verified that the first three nibbles correspond to the tag's lock configuration. The TID reported by our Washington State EDLs is **E2 00 10 50**, which corresponds to an $E2_h$-class Impinj Monza chip.

To confirm that these TIDs do not confer anti-counterfeiting protection, we have cloned both a Passport Card and a Washington State EDL onto commercially-available, off-the-shelf tags from the same manufacturers as the originals. By *cloned*, we mean that the EPC and TID values are reported identically by the clone tags.[2] Additionally, we inferred the lock state of both card types and duplicated that as well. Provided that the Passport Card or Washington State EDL do not implement additional, undocumented functionality, the only contents that we were unable to clone were the ACCESS PIN on both cards, and the KILL PIN of the Passport Card. The TID therefore does not serve as the basic anti-cloning tool as envisioned by DHS. One explanation for this might be the fact that, via personal communications, the DHS has informed us that they learned of the existence of tag-unique TIDs too late to be incorporated into these cards.

We further maintain that the characterization of the full, tag-specific TID as a powerful anti-cloning tool is overly sanguine in the long term. While such tag-specific TIDs may prevent simple copying of one EPC into another, it does not prevent the *emulation* of an EPC tag in another radio device. In other words, the TID may (or may not) help prevent *physical* copying of an EPC tag, but it certainly does not prevent *logical* copying.[3] An ordinary RFID reader makes no distinction between a tag embodied in a flake of silicon and one emulated by a larger, more powerfully instrumented platform.

A number of general-purpose tag emulation platforms such as OpenPCD [34] and the RFID Guardian [35] already exist for HF tags. It is just a matter of time before similar tools emerge for Gen-2 EPC tags. The Intel WISP [41], for instance, is a physically compact RFID platform with a fully programmable microprocessor that operates in the UHF domain as a Gen-1 EPC tag. Release is planned in the near future of Gen-2 EPC WISP. Thus, emulator devices are likely to be broadly accessible in coming years.

The decision to forego the security offered by the TID in the Washington State EDL and Passport Card thus increases the short-term risks of cloning, as it eliminates a basic protection against the straightforward copying of publicly viewable values into a fresh Gen-2 tag. In the longer term, commercially-available emulator devices may reduce the protective value of tag-specific TIDs. That said, the TID may still have some longer-term value as a countermeasure to easy cloning of EDLs and Passport Cards into devices with the same form factor, i.e., Gen-2-equipped cards.

[2]However, cloning a tag's EPC and TID may not be sufficient for an adversary's purposes; e.g., in some cases an adversary may also need to produce a false card itself.

[3]There are well documented, low-cost attacks against smartcards, which possess tamper-resistance features well beyond those of EPC tags; see, e.g., [6]. It therefore seems probable that an attacker with modest resources can use physically invasive techniques to alter the data in an EPC tag. And if only one manufacturer makes Gen-2 tags available with programmable TIDs, they can act as clones for *any* manufacturer's tags.

3.2 Other memory banks

Assuming the Gen-2 tags in the EDL and Passport Card are identical to the commercial, off-the-shelf tags indicated by their TID, the only read-protected piece of memory on the cards is the KILL PIN on the Passport Card, and the ACCESS PIN on both. We have experimentally verified that the entire EPC memory bank (which contains the card's unique EPC value) is readable, as is the TID memory bank. The Impinj Monza chip does not have a User memory bank, and the Alien Higgs-2 chip only uses a User memory bank when the KILL and ACCESS PINs are not used [28]. We have also verified that the cards report a "no such memory location" error when attempting to read words we do not expect to be present (such as the User memory bank).

3.3 Kill-PIN selection

The KILL PIN is unprogrammed and not locked on the Washington State EDLs. We have verified that we can directly write this 32-bit KILL PIN. We have not verified that we can in fact kill an EDL (an experiment that would be detrimental to its owner). We have verified our ability, however, to kill a cloned EDL with an identical Gen-2 tag model, an Impinj Monza, over the air. Thus, unless the Washington State EDL Gen-2 tag is specially manufactured—which seems unlikely, given the presence of a generic TID—it is subject to over-the-air killing by any reader.

Alternatively, an attacker can exploit the KILL PIN as a covert channel. She can set it as desired, thereby "marking" the EDL bearer with a 32-bit value accessible to any other reader.

3.4 Read-range experiments

Read ranges are a major determinant of the vulnerability of an EDL or Passport Card to clandestine cloning attacks, as well as attacks against privacy. As explained above, a single scan of a tag in either type of identity document is sufficient to create a clone. In an attempt to mitigate resulting privacy concerns, the United States Department of State provides radio-opaque shielding sleeves with each Passport Card. These sleeves attenuate the distance at which a card may be read. Similarly, Washington State is making protective sleeves available to holders of its EDLs.

It is uncertain that EDL and Passport Card bearers will consistently use their protective sleeves. These documents require security hygiene beyond that of other commonly carried cards, demanding from bearers heightened vigilance and tolerance of inconvenience. In section 5.1, we briefly examine the relevant literature on the psychology of fear appeals. This body of research suggests that the abstract warnings accompanying EDLs and Passport Cards, e.g., the injunction on the Passport Card sleeve that, "Your Passport Card should be kept in its protective sleeve when not in use," may be relatively ineffective in stimulating sleeve use. Additionally, as shown recently by King and Mcdiarmid [25], most bearers do not have accurate mental models of RFID privacy and security, and are therefore ill-equipped to make informed decisions about tag management.

The effective read ranges of protected and unprotected EDLs and Passport Cards in everyday environments therefore both have a strong bearing on the overall security of the border-crossing system, as well as on the privacy of people with these cards.

While deployers of Gen-2 EPC tags typically cite a reli-

Figure 1: The sleeves used for our shielded distance tests. The crumpled sleeve is in the foreground, with the new sleeve behind it.

able operational range of tens of feet [39], read ranges can vary considerably as a function of the material to which a tag is affixed, the configuration of the interrogating reader, and the physical characteristics of the ambient scanning environment.

We evaluated the read range of the Passport Card and Washington State EDL in several different physical environments, namely: (A) Indoors, freestanding, but with other objects nearby; (B) Indoors, in a corridor, with no other nearby objects; and (C) Outdoors in freespace. In all environments, we also evaluated various ways of carrying the cards, namely: (1) Held away from the body; (2) Inside a purse; both inside a wallet and in a side pocket; (3) In a backpack; (4) In a wallet in a back trouser pocket; (5) In a wallet in a front shorts pocket; and (6) Adjacent to a wallet in a front shorts pocket. The wallet contained 14 magnetic stripe cards, two non-magnetic stripe plastic cards, nine paper cards, and approximately six dollar bills.

To evaluate the effectiveness of radio-opaque protective sleeves, we measured the maximum read range in a variety of situations, namely: (i) In a new sleeve, held out by hand; (ii) In a crumpled sleeve, held out by hand; (iii) In a new sleeve, in a wallet in a back trouser pocket; and (iv) In a crumpled sleeve, in a wallet in a back trouser pocket.

We used Secure Sleeves^{TM} from Identity Stonghold, the manufacturer supplying sleeves for both the Passport Card and the Washington State EDL [1, 43, 44]. The sleeves are shown in Figure 1. We do not expect the ambient environment to impact the read ranges in these tests, as the ranges are relatively short, so all shielded experiments were performed in the lab. We also experimented with the EDL in a sleeve obtained from the State of Washington and with the Passport Card in a sleeve obtained from Passport Services, and we report on these experiments as well.

To perform these experiments, we used an Impinj Speedway R1000 reader, with a Cushcraft S9028PCL circularly-polarized antenna. The effective radiated power of the antenna was 36 dBm, the maximum allowed by the FCC. The center of the antenna was 88 cm off the ground, and the cards were placed directly in front of the antenna. We measured the maximum distance at which we could read the cards when held in place for up to five seconds. We report these maximum distances in Table 1 (unshielded), Table 2 (shielded with the purchased Secure Sleeves^{TM}), and Table 3 (shielded with the sleeves provided for use with the respective cards).[4]

	New Sleeve		Crumpled Sleeve	
	EDL	**PC**	**EDL**	**PC**
Freespace	20 cm	No Reads	29 cm	34 cm
Back wallet	27 cm	No Reads	57 cm	No Reads

Table 2: Maximum read range in a Secure Sleeves^{TM} shielded sleeve

	New Sleeve		Crumpled Sleeve	
	EDL	**PC**	**EDL**	**PC**
Freespace	62 cm	No Reads	63 cm	No Reads
Back wallet		No Reads		No Reads

Table 3: Maximum read range in shielded sleeve provided for use with the specific cards; at the time of this writing the wallet was not available for us to complete the measurements with the provided sleeve and the EDL in a wallet

Remarks. An RFID tag has not a single read range, but in effect has multiple "read ranges," depending on the operational scenario [22]. The range of main interest in most (benign) cases is that at which a reader can directly interrogate a tag. In a security context, though, the "eavesdropping range" is another of interest. This is the distance from which a rogue reader can intercept the reply of a tag to a legitimate, interrogating reader. Eavesdropping is feasible at a much greater distance than direct tag interrogation, as the eavesdropping reader need not be close enough to the tag to power it. Eavesdropping is also a passive activity, undetectable by radio-monitoring devices. Eavesdropping on an EDL or Passport Card interrogation is sufficient to enable successful cloning as well as privacy attacks. We have not yet conducted experiments on the eavesdropping ranges for EDLs and Passport Cards. Such experiments would at present require specialized firmware or equipment, as eavesdropping is not supported by off-the-shelf commercial readers.

4. DEFENSIVE DIRECTIONS

4.1 Backward-compatible defenses against cloning

The Class-1 Gen-2 specification has no explicit anti-cloning features [19]. For this reason, Juels [21] proposes the co-opting of two Gen-2 access-control commands for authentication of tags, summarized as follows:

1. The KILL command. KILL is an EPC feature designed to protect consumer privacy by allowing tags to be disabled at the point of sale in retail environments. As a mandatory part of the standard, KILL is implemented (to the best of our knowledge) in all Class-1 Gen-2 EPC tags. When a tag successfully receives the KILL command along with a tag-specific 32-bit KILL PIN P_{kill}, it becomes perma-

[4]In a few situations, we exhausted the space available to us in our experimental environment—i.e., backed ourselves into a wall—before we could find the maximum distance. These situations are denoted with a +.

	In Lab		In Hallway		Outdoors	
Scenario	**EDL**	**PC**	**EDL**	**PC**	**EDL**	**PC**
Freespace (Held Out in Hand)	530+ cm	530+ cm	4950+ cm	4950+ cm	788 cm	720 cm
Wallet in Purse	277 cm	528+ cm	1125 cm	276cm	586 cm	46 cm
Purse Side Pocket	528+ cm	528+ cm	4950+ cm	4950+ cm	833 cm	190 cm
Wallet in Back Pocket	253 cm	57 cm	193 cm	62cm	182 cm	58cm
Wallet in Front Pocket	270 cm	244cm	886 cm	65cm	240 cm	192cm
Next to Wallet in Front Pocket	417 cm	320 cm	4950+ cm	1137 cm	833 cm	580 cm
Empty Backpack	528+ cm	528+ cm	4950+ cm	4950+ cm	1050 cm	982 cm

Table 1: Maximum read range in a variety of situations

nently inoperative. Tag disablement, however, is a power-intensive operation. When a reader transmits the KILL command with power sufficient for the tag to respond, but not to disable itself, the tag replies with a *Not Enough Power* response. In this type of low-power session, a side-effect is that the tag *also* indicates the correctness or incorrectness of the PIN transmitted by the reader.

Co-opting KILL for tag authentication. A reader with knowledge of P_{kill} can authenticate a tag by constructing an invalid PIN P'_{kill} and transmitting the pair (P'_{kill}, P_{kill}) in a random order across two low-power kill command sessions. A valid tag will acknowledge the correct PIN and reject the incorrect PIN; an invalid one can respond correctly with probability at most 1/2. We refer to this idea as *KILL-Based Authentication* (KBA).

While a detection probability of 1/2 is not high for an individual tag, it is high enough for detection of cloning on a systemic basis. Also, by transmitting $N-1$ spurious PINs and one legitimate one, at a linear cost in authentication time, a reader can boost its probability of detection of an invalid tag to $1 - \frac{1}{N}$.

The challenge of KBA, and the one we investigate below, is the reliable transmission of commands in the low-power regime of a target tag. Too much power, and the tag will be killed.[5] Too little, and the tag will not respond. To the best of our knowledge, KBA has remained a research proposal, and not yet seen empirical study.

2. The ACCESS command. EPC tags can carry secret data D with read-access control. Such data are readable only through use of the ACCESS command, with an accompanying tag-specific 32-bit PIN P_{access}. The KILL PIN itself is one such piece of read-protected data.

Co-opting ACCESS for tag authentication. An entity with knowledge of P_{access} for a tag as well as D can authenticate the tag by checking D. An entity without knowledge of P_{access} cannot extract D without physically attacking the tag. This mode of authentication is a kind of one-time challenge-response that we refer to as *ACCESS-based authentication* (ABA).

We performed a quick experiment to determine whether ABA would impact read range. We used a new Impinj Monza tag for this experiment. We first determined the maximum read range of the tag outdoors (as in Section 3.4). We then programmed P_{kill} and P_{access} onto the tag, locked them against unsecured reading or writing, programmed the reader to use P_{access} to read P_{kill}, and again measured the maximum read range. For our particular tag, we found a maximum read range of 475 cm in both instances, suggesting that ABA should not significantly impact read ranges.

Variants are possible. For instance, without the presence of a secret D, a form of weak ABA is possible in which P_{access} is used in the same mode as KBA, i.e., tested through embedding in a set of spurious PINs. This weak ABA is the only form that would seem generally viable in today's EDL / PASS infrastructure. Passport Cards carry secret data D in the form of P_{kill}, but EDLs, as noted above, do not have their KILL PINs set.

A stronger variant is possible as a form of crude rolling code created by overwriting D with a new random value D' on each authentication and storing this new value in a back-end system. (While an attacker could sniff D' and continue using a cloned card, once the legitimate card was read, the duplication of D' would be discovered.)

Advantages and limitations. Both KBA and ABA have advantages and disadvantages. KBA is of interest for two reasons. First, ACCESS is an optional, not a mandatory command in the EPC standard, so tags need not in principle support it. Second it is possible to deploy the ABA and KBA independently. One entity can use P_{kill} to authenticate tags using KILL, but cannot perform tag cloning against a second, more privileged entity with knowledge of P_{access}. For example, P_{kill} might be revealed to state law enforcement officials, allowing them to authenticate tags (and kill them), but not to clone them.

Neither technique, of course, is resistant to eavesdropping. They are ad-hoc tools meant to allow authentication in the absence of cryptography or other supporting features. The most compelling feature of KBA and ABA (where available) is their backward compatibility. Neither requires any modifications to already deployed EPC tags. Finally, KBA, if not carefully implemented, may in some cases actually kill the cards.

4.2 Experiments in KILL-based authentication

To evaluate the viability of KILL-based authentication (KBA) we explore the design space of possible KBA algorithms. As we have explained, the implementation challenge of a KBA algorithm is to calibrate the transmit power of a reader such that it can interrogate tags freely, but does not give the tags enough power to kill themselves.

[5]As an alternative to power-calibration, [21] also proposes the manufacture of tags in which KILL always operates as if in the low-power regime, i.e., in which a manufacturer sacrifices KILL as a privacy feature in exchange for KBA. However, this would be a violation of the EPC Gen2 standard.

Distance	Successful auths	Kills
40cm	0	10
50cm	6	2
60cm	9	1
70cm	7	0
80cm	9	0
90cm	6	0
100cm	10	0
110cm	8	0
120cm	10	0
130cm	9	0
140cm	9	0
150cm	9	0
160cm	8	0
170cm	9	0
180cm	7	0
190cm	9	0
200cm	9	0

Table 4: Simple KILL-based Authentication

As a first step, we consider a simple algorithm in which a reader ramps up power until it receives a response from a tag. In particular, our implementation ramps up the reader's power from 15 dBm to 30 dBm (the full range of our reader) in 0.25 dBm increments (the minimum supported by our reader), transmitting a KILL command at each power level in turn. (Our antenna provides an effective 6 dB gain.) When the reader successfully receives a reply from the target tag, the power level is fixed. The reader then sends a total of N KILL commands, with $N-1$ bogus PINs, and 1 real PIN. We tested this algorithm with a tag placed at distances of 40 cm to 200 cm from the antenna, in 10 cm increments. For our tests we set $N = 10$; we repeated the algorithm 10 times at each distance. All experiments were performed with the same setup that we used in our distance tests (see section 3.4). If despite the initial power calibration, a tag did not consistently respond across the authentication session, we treat the authentication attempt as unsuccessful. We report the number of successful authentications and unintentional KILLs in Table 4.

The simple power-ramping algorithm unfortunately has a notable weakness: If the tag is too close, the reader power cannot be adjusted to a low enough level to avoid killing it. These unintended kills aside, the algorithm proves fairly robust, successfully authenticating tags a majority of the time. (In practice, of course, an authentication attempt could merely be repeated if unsuccessful.) A reader with support for lower-power emission could in principle support shorter-range KBA.

A good KBA algorithm should be robust enough to support a wide variety of reader characteristics. With this principle in mind, we developed a more sophisticated KBA algorithm that tries to avoid unintentional kills by ensuring a sharp separation between the power levels required for read and write operations and carefully calibrating its power between these two levels. We refer to this algorithm as *scaled KBA*. Scaled KBA involves a calibration phase with five steps:

1. By means of power ramping, determine the minimum reader power level PWR_R required to read the target tag.
2. By means of power ramping, determine the minimum reader power level PWR_W required to write to the tag.
3. Verify the availability of minimum margin $PWR_W - PWR_R \geq \mu$, where μ is a minimum power-margin parameter. If not, abort.
4. Scale the reader's power level within the range $PWR_R + \delta(PWR_W - PWR_R)$, for $\delta \in [0, 1]$.[6]
5. Ensure that the power level selected doesn't allow a tag to write to itself.

Note, however, that steps 2 and 5 require writing to the tag. One potential option is to temporarily overwrite part of the tag's EPC value. We used this technique and performed these tests with our own tags. This technique will not work on cards where all memory is permalocked read-only (such as the Passport Card).

After some cursory tuning, we adopted $\mu = 2dBm$ and $\delta = 1/4$ in our experiments. As in the simple KBA algorithm, we incremented the power of the reader from 15 dBm to 30 dBm in 0.25 dBm increments, and let $N = 10$. We evaluated this algorithm at distances from 10 cm to 200 cm from the antenna, in 10 cm increments.

We executed the scaled KBA algorithm 100 times at each distance. Table 5 reports the number of successful authentications at each distance. We also report authentication failures due to detection of a power margin below μ, to a failed write test (where the the tag's EPC value is temporarily changed when it shouldn't be), or to an accidental kill. Other authentication failures occur when the tag fails to respond with an "insufficient power" code on the correct PIN. This can be caused by a number of factors, from RF noise, or to the tag not having enough power to correctly execute its state machine. These results are summarized in Table 5. We report power and timing measurements in Tables 6 and 7 in the appendix.

We see that the scaled KBA algorithm achieves its objective of reducing (and seemingly eliminating) unintentional kills at short range. Table 6 is especially informative: If the minimum read level is above 16 dBm, there is always at least a 2 dBm margin between the mean minimum read and write power levels.

The scaled KBA algorithm does, however, produce a small rate of unintentional killing in the range of 130–150cm. The reason is unclear. (Multipath effects, for instance, can introduce unpredictable phenomena into wireless environments.) In well controlled physical environments, e.g., in an "authentication chamber" at a border crossing, however, we believe it would be possible largely to eliminate the power fluctuations that cause unintentional killing. Indeed, in such environments, the simple KBA algorithm might itself be effective. Reducing N or disregarding failed responses to spurious PINs, with an appropriate adjustment in authentication confidence, would also help.

We believe that the best and most robust approach to the problem of unintentional killing, however, is to constrain the power delivered to a tag by modifying the reader protocol.

[6]Of course, more sophisticated scaling functions are possible.

Distance	Auths	Margin Failures	Write Test Failures	Kills
10cm	0	100	0	0
20cm	0	99	1	0
30cm	0	100	0	0
40cm	0	100	0	0
50cm	0	99	1	0
60cm	98	0	0	0
70cm	91	5	0	0
80cm	96	1	0	0
90cm	91	0	0	0
100cm	88	4	7	0
110cm	63	18	14	0
120cm	58	29	12	0
130cm	62	8	2	1
140cm	50	43	4	1
150cm	84	2	2	2
160cm	83	4	7	0
170cm	88	2	0	0
180cm	89	0	0	0
190cm	89	2	0	0
200cm	83	10	4	0

Table 5: Scaled Timing and Reliability Results

In particular, we suspect that an abrupt cutting of a reader's emission in the course of a KILL command might put a tag reliably in the low-power regime. Such approaches, however, would require modification to reader firmware and/or hardware. We therefore reserve them for future work.

In summary, our experiments show that KBA authentication is a viable technique, and thus an attractive complement or alternative to ABA for off-the-shelf EPC tags.

Remark. As we have noted, the write operation is not a mandatory feature in Gen-2 tags. It is interesting to observe, however, that our scaled KBA algorithm only attempts authentication when the minimum power level is above 16 dBm. For tags that do not support the write operation, therefore, a variant of our simple KBA algorithm that first checks that the minimum read-power level is 16dBm would merit investigation. Since Passport Cards are permalocked read-only, this variant seems like the most promising approach if KBA is to be integrated.

4.3 Protecting privacy

Passport Cards and EDLs present a risk of clandestine tracking of bearers based on the uniquely identifying data they contain. Many already deployed and commonly carried RFID tags already present much the same risk, including RFID-enabled credit cards, proximity cards, and automobile ignition keys. Similarly, mobile handsets are subject to secret tracking, by means of both their cellular signals and their secondary wireless interfaces, such as Bluetooth and WiFi.

EPC tags, however, present a somewhat distinct privacy problem. As our experiments show, their read range considerably exceeds that of other common RFID tags. High-frequency and low-frequency tags are vulnerable to clandestine interrogation only at short range—generally no more than a meter [22]. Additionally, the EPC tags in Passport Cards and EDLs are identifiable as such (their EPC values have a common prefix), and therefore reveal potentially significant personal information. For example, as Washington State is the one of only two states thus far to issue EDLs, and the EPC tags in its drivers' licenses are distinct from those in Passport Cards, it is possible to identify a (probable) resident of Washington State surreptitiously by means of her EDL. The RFID tags in other items, like credit cards, are similarly identifiable, but again, their read range is rather more limited.

Given the EPC tags also differ from other long-range radio identifiers (such as cellular, Bluetooth, and WiFi signals) in that it is fairly plausible that large EPC-reading infrastructures will be set up for item-level tracking. Additionally, there may be cases where people will have their Passport Cards or EDLs on them but not other computational devices.

A central issue created by the lack of privacy with EPC-tagged identity documents is the increased risk of cloning based on clandestine scanning. The best way to protect against this threat is to incorporate higher-cost RFID tags that support strong cryptographic authentication. United States e-passports, as noted above, carry cryptographic protections which, while imperfect in several respects [23], probably afford adequate protections against cloning and attacks on privacy for most bearers.

Given the choice by the Department of Homeland Security and the Department of State to incorporate EPC tags into EDLs and Passport Cards respectively, KBA and/or ABA can serve as weak stand-ins for cryptographic authentication, with no impact on tag cost. KBA does, however, impose shorter operational ranges than reading, and might therefore be best deployed on a selective basis, perhaps as part of the final confirmation of passenger identities at the border. While we have reason to believe ABA does not affect operational read ranges (see Section 4.1), given the vulnerability of both techniques to eavesdropping, short-range, low-power operation might be the preferred mode of use in any case.

Protection of tag privacy itself confers protection against cloning. Researchers have proposed a number of techniques for protecting tags against unwanted scanning, some of which need not significantly undermine the cost and range characteristics of EPC tags.[7] Among the techniques applicable to privacy protection in identity documents are:

- **On/off sensors:** A light sensor can block data release by an EPC tag inside a wallet or purse; conversely, a push button might require a holder intentionally to activate an identity document for scanning. Capacitive sensing [12] can detect the touch of a bearer as a form of authorization.

- **Motion sensors / secret handshakes:** Heydt-Benjamin et al. [17] suggest the use of sensors to detect certain bearer motions as prerequisites for data release, e.g., a "tap-and-go" gesture for a credit card. Czeskis et al. [12] expand on this idea and actually demonstrate a practical, passive tag whose motion sensor authorizes

[7] Fishkin et al. [13] propose a clever and potentially inexpensive approach to privacy protection in which a tag estimates the physical distance of an interrogating reader and discloses data selectively. Unfortunately, given the need for long read ranges in ordinary use, we see no way to apply this technique to the problem of identity-document protection.

data release only on execution by the bearer of an assigned gesture, such as the waving the tag in front of the reader.

- **Blocker tags:** Proposed in [24], blocker tags offer an alternative to protective sleeves. Comparable in form and cost to an ordinary tag, a blocker tag prevents the scanning of other, nearby RFID tags. An EPC-specific blocker tag might be carried in a wallet or purse alongside EPC-tagged identity documents. In this case, removal of an identity document for presentation might automatically separate it from the blocker and enable it to be scanned—without the inconvenience of a protective sleeve.

5. RFID AT THE BORDER: A CASE STUDY SECURITY APPLICATION OF RFID

DHS includes the U.S. Customs and Border Protection agency, and is thus responsible for the logistics around border control. While DHS has not disclosed the precise procedure for border crossing using a Passport Card or EDL [29], we can glean a basic outline from sources such as [3, 5, 31]. Given the partial disclosure of border crossing procedures, we stress that part of the discussion below is speculative. Nevertheless, we believe that the lessons learned from these discussions could be useful in U.S. border crossing scenarios, as well as in other RFID deployment scenarios, including border crossing scenarios in other countries seeking to deploy similar technologies.

1. **Radio presentation of cards:** As a passenger vehicle approaches the checkpoint, the passengers place their Passport Cards / EDLs on the dashboard. If the passengers keep their cards in protective (Faraday-cage) sleeves, then they remove those cards from the sleeves first. (The long read range of Gen-2 tags supports this procedure.)

2. **Scanning and database querying:** A reader scans the cards and extracts their identifiers. These identifiers are used to reference passenger dossiers in a federal database and display their contents to a border control agent.

3. **Confirmation:** The border control agent visually verifies the correspondence between the database photos and passengers.

Whether the border control agent will physically inspect the identity documents of all passengers has not been publicly disclosed, nor has the policy governing interviews of passengers. Any of several factors, however, might prompt a border-control agent to interview passengers or inspect their cards, e.g., a seeming mismatch between the database photo of a passenger and her appearance, the presence of a passenger name on a watchlist, etc. Our personal communications with DHS suggests that border crossing agents may inspect the physical documents of all travelers.

It is possible (although unlikely in our view) that DHS has implemented weak ABA for Passport Cards and EDLs, or ordinary ABA just for Passport Cards. This countermeasure would help combat the risk of cloning of cards. We are unable to ascertain based on our experiments whether or not such a countermeasure is in place.[8] Given that the KILL PIN is not set in the Washington State EDL, it seems likely that no kill-based authentication takes place.

5.1 Operational risks

We now discuss three potential systemic risks around Passport Cards and EDLs resulting from the vulnerabilities in their EPC tags.

5.1.1 *EPC data and cognitive biases in passenger screening*

The DHS border-crossing protocol threatens to create a new and significant cognitive influence on the passenger screening process based on the authenticity of EPC tags. As we now explain, three well-documented cognitive phenomena suggest this risk: *automation bias*, *primacy effects*, and *vigilance decrement*.

The function of EPC-tag scanning is to flag travelers on watchlists automatically as an initial decisional indication to border control agents—through the scanning and database querying step of the screening process mentioned above. Research on human factors in aviation systems documents a significant bias in human decision-making in response to automated cues, a phenomenon known as *automation bias*. In a study involving simulated flight tasks, for instance, Skitka, Mosier, and Burdick [40] find that automated decision recommendations around the discharge of a given task reduce the vigilance of human operators. They note that, "The presence of automated cues appears to diminish the likelihood that decision makers will either put forth the cognitive effort to seek out other diagnostic information or process all available information in cognitively complex ways.ŠŠ

The accuracy of the initial watchlist flagging process hinges entirely on *whether or not a scanned EPC tag is authentic*. A counterfeit tag will point to an inaccurate traveler record. Thus, while the passenger screening operation potentially involves multiple stages of validity checking, the authenticity of EPC tags promises to exert a significant influence over border-agent decision making.

This influence occurs at the critical, first stage of the screening process. The function of EPC-tag scanning is to identify passengers on watchlists *before* the border-control agent interacts with them. (In contrast, when EPC tags are not present, the border agent receives essential cues as to passenger validity *prior* to critical stages of the decision making process: When performing manual handling of identity documents, an agentŠs first point of interaction is with passengers and identity documents themselves.) Consequently, the adoption of EPC-driven screening creates new scope for automation bias through the entire screening process.

The EPC-dependent watchlist check on passengers is also likely to weigh disproportionately with a border agent because of a psychological phenomenon known as the *primacy effect*. When people draw conclusions on the basis of information acquired and integrated over time, the information acquired early in the process typically carries more weight than that acquired later [38, 26]. When a border agent is informed at the beginning of the screening process that the

[8]It would be possible to determine whether ABA takes place at the border by recording a reader-tag interrogation and analyzing a transcript. A would-be attacker could perform this procedure passively and therefore without detection, i.e., without emitting a radio signal.

passengers in a vehicle are not on any watchlist, the primacy effect predicts a priming toward a lower state of alertness.

The rarity of watchlist sitings is another reason to anticipate sub-optimal levels of border agent vigilance in the face of automated cues. The number of travelers present on the TSA no-fly list includes a small fraction of the traveling population [42]. It seems probable that watchlists at land and sea ports will be similarly limited. Research on people performing source monitoring for rare, unpredictable targets—such as airport security screeners examining baggage for weapons—has confirmed a cognitive phenomenon known as *vigilance decrement*. As people grow habituated to benign stimuli over time, their accuracy and speed of detection deteriorates [11].

It is possible that DHS has studied the effects of automation bias, primacy effects, and vigilance decrement and sought to embed compensating elements in the border-crossing protocol. The cloning vulnerability of EPC tags, however, clearly creates a security environment with a critical—and in our view, fragile—dependence on unfavorable psychological conditions.

5.1.2 Challenges in protective-sleeve acceptance

Research on public-health campaigns has long documented the essential nature of fear appeals in stimulating protective behavior. The perceived probability and severity of a threat are key determinants of whether the public will adopt proposed protective measures [47]. Not surprisingly, empirical studies show that that strong fear appeals produce high levels of perceived severity and susceptibility, while low or weak fear appeals do not [49]. Additionally, research has clearly established that people respond to concrete scenarios and threats more than abstract ones [9].

The warnings on protective sleeves and associated materials for Passport Cards and WA EDLs are abstract, rather than concrete; they do not convey a strong fear appeal. The Washington State Dept. of Licensing notes that, "The sleeve protects the Radio Frequency Identification (RFID) tag in your Enhanced Driver License/ID Card from being read when the card isn't being used for border crossing" [32]. The reverse side of the Passport Card simply states, "Your Passport Card should be kept in its protective sleeve when not in use."

We believe that these messages will result in low levels of sleeve use, particularly given the benefit of convenience in non-use [37].[9] An effective educational campaign would need to alert people to a serious, specific risk associated with non-use of sleeves. (E.g., "if you don't use your sleeve, there's a serious risk that a criminal will skim your card and steal your identity.") It seems unlikely that government agencies will draw attention to such specific vulnerabilities in the WHTI system or to advertise security breaches. Without such specificity, though, there is a risk of public habituation and complacence over time [10] resulting in low use of sleeves.

5.1.3 Design drift

Second, there is the risk of what we call *design drift*. In its specification of e-passport standards [18], International Civil Aviation Organization (ICAO) noted the possibility of e-passports application being extended to authentication in commercial settings. If EDLs or Passport Cards see use outside the specially constrained setting of border crossing, extreme care will be required. Given the many uses of drivers licenses today, e.g., age-identification for liquor purchases, gradual use of their EPC tags for new applications—i.e., mission creep—is easily conceivable. Further, additional uses of the EDL and Passport Cards might evolve outside of the U.S., particularly if other countries adopt similar technologies.

The use of EPC tags in EDLs is itself an example of design drift and its dangers. The first concrete design and implementation of the technology was for the Passport Card. Roll-out to EDL programs, such as that of Washington State, took place subsequently [33]. We noted above the vulnerability created by unlocked "kill" PINs in the Washington State EDL, as well as the susceptibility to clandestine scanning through a protective sleeve. These deficiencies may well have arisen due to a lack of comprehensive technical criteria by U.S. agencies.

Additionally, Passport Cards and EDLs will probably see different modes of use. As a newly created form of document for relatively infrequent use, the Passport Card may inspire its bearers to exercise special security precautions, like use of a protective sleeve. In contrast, many holders of drivers licenses carry them at all times in their wallets, and have done so for years without any special protective measures. Given how frequently people handle them and the long established patterns of use for drivers licenses, it is difficult to imagine that bearers will consistently use their protective sleeves. Moreover, there are legitimate use cases for drivers licenses that will require their owners to remove them from the protective sleeves, such as when making certain purchases, checking into hotels, or entering bars.

5.2 Specific threats

5.2.1 Illegal border-crossing via counterfeiting

In principle, even if border control agents do not physically inspect cards, visual inspection of passengers offers a check against cloning. In effect, the border control agent biometrically authenticates passengers (performs face recognition) by visual inspection. As acknowledged by DHS in its Privacy Impact Assessment, however, there is a risk of impostors stealing identities from victims with similar physical appearances [31]. It seems likely that passengers will in many or most cases not need to disembark from their vehicles. Thus, suboptimal lighting conditions are to be expected, and secondary cues like passenger height may be intelligible to border-control agents.

Of course, it is possible to create counterfeit conventional drivers' licenses or passports or duplicate these identity documents without exploiting their EPC tags. The presence of EPC tags, however, creates two new vulnerabilities:

- **Remote cloning:** EPC tags eliminate the need for an attacker to obtain physical possession of a card in order to clone its electronic contents. A single clandestine read suffices. (Use of some form of ABA at U.S. borders, if present, would help alleviate this risk.)

- **Clandestine victim profiling:** The read range of EDLs and Passport Cards is long enough for an at-

[9]While the owners of the three identity cards we used in our experiments have a personal and professional interest in privacy issues, they in fact misplaced their sleeves.

tacker to monitor bearers' movements and target victims according to their patterns of border crossings.

We illustrate these vulnerabilities with an example:

A human-smuggling ring aims to bring illegal aliens into the U.S. from Mexico. The smuggling ring hides card readers and cameras in highly frequented locations near the U.S.-Mexican border, e.g., bars, convenience stores. It monitors and records the identifiers in EDLs and Passport Cards, as well as photos of their bearers. To identify a victim whose card is to be cloned for a target imposter, the ring: (1) Identifies close matches between the imposter and the victims in its roster, and (2) Selects a victim among these matches that has been seen recently on the Mexican side of the border. (Two crossings into the U.S. without a corresponding crossing into Mexico might trigger heightened scrutiny.)

If the impostor's card is not physically inspected, the forged card need not carry a valid photo or even resemble a true identity document. As a human-smuggling operation need not achieve more than a reasonable probability of success, this attack would be broadly successful provided that cards are not consistently subject to careful physical inspection. As an additional scenario, anyone who is currently able to physically manipulate a card (e.g., a hotel's check-in attendant or a bartender) could clone both the physical and electronic representation of the card.

5.2.2 Denial-of-service attacks

Our study suggests that anyone with a Gen-2 reader near a Washington State EDL can permanently disable the RFID chip without authorization; see section 3.3.

One of the benefits of EDLs is improved convenience for border crossings. Disabling an EDL would naturally nullify this benefit. Worse still, border crossings agents will likely not expect to encounter EDL cards with disabled RFID components and hence will likely spend *more* time interacting with a person attempting to cross a border with a disabled EDL than with a person attempting to cross the border with a traditional passport. This leads to at least three classes of scenarios in which an attacker might wish to leverage the EDL's vulnerability to cause havoc: attacks against targeted individuals, malicious pranks against random individuals, and attacks against the entire border crossing system.

We again illustrate these vulnerabilities with an example, though stress the other examples abound:

There will soon be massive border crossings between Washington State and Canada for the 2010 Olympics in Vancouver, BC. An attack on the efficiency of these border crossings could cause serious disruption. One could easily imagine a large-scale denial-of-service attack against these cards at the 2010 Vancouver Olympics. For example, an attacker could set up an RFID reader to kill any EDLs it sees near the venue's entrances. An attacker could also place malicious readers near the key rest facilities and other nearby locales.

The Departments of State and Homeland Security point out that the EDLs and Passport Cards have Machine-Readable Zones that can still be processed if the RFID tag cannot be interrogated. However, this contradicts a statement made by the State of Washington in their EDL FAQ, which states that "tampering with or deactivating the RFID tag embedded in your EDL/ID will invalidate the card so it cannot be used for border crossing [32]."

5.2.3 Other scenarios

We stress that there are other examples of how one might abuse the current properties of the EDL and Passport Cards. For example, an attacker might place a doctored Gen-2 tag on the dashboard of a victim's car. This Gen-2 tag could be the clone of the EDL of another person, thereby potentially causing the victim extra hassle at the border.

The purpose of this section is not to exhaustively describe all possible risks associated with the current EDL and Passport Card implementations, but to merely survey the potential threat landscape. We would be remiss, however, not to remark once again about the privacy concerns associated with the use of persistent and easily readable identifiers on the EDLs and Passport Cards. Even though the EPC values on these cards do not reveal the owner's name *directly*, there are many straightforward *indirect* methods for exploiting these EPC values to compromise an individual's privacy and safety. The risk of using persistent identifiers is indeed well known, as exemplified by the many works highlighting the same risks with other technologies, e.g., [15, 20, 22, 36]. The privacy concerns are amplified for the EDLs and Passport Cards because of their long read ranges and because of the fact that, contrary to what most users would expect, these cards can in some cases be read even when in protective sleeves.

5.3 Recommendations

We recommend several practices to reduce the risk of use of cloned EPC-enabled identity documents in illegitimate border crossings or other settings. We believe that the following four recommendations are implementable in the short-term.

1. **Photo comparison:** The photo in a Passport Card or EDL may be regarded as a piece of secret data, albeit a weak one. As we have shown, an attacker can skim and clone the EPC tag of a card while it is hidden. The corresponding photo can only be accessed by means of direct visual contact. Thus, a card cloned by means of remote skimming will contain a discrepancy between its photo and the one registered in the passenger database. An attacker can try to construct a photo based on the face of the victim, but an astute border-control agent, or an automated checking procedure should be able to detect differences. If border control agents do not normally take physical possession of identity documents, this procedure of comparison might at least serve as a form of spot checking.

2. **Set the KILL PIN on EDL cards:** We recommend that Washington State immediately move to set the KILL PINs on the EDLs it issues.

3. **Enable per-card TIDs on the EDL and Passport Cards:** We recommend that both the EDLs and the Passport Cards use individualized TIDs for each card. We stress, however, that the use of individualized TIDs should only be seen as a *temporary* and *incomplete* measure to make it harder (but still far from impossible) to clone an EDL.

4. **Random testing:** We suggest that border agents adopt a strategy similar to that used by airline security screeners: Train customs officials in how to respond to

cloning and killing attacks by randomly sending undercover agents across the border with cloned or killed EDL or Passport Cards.

We additionally make the following longer-term recommendations:

1. **Anti-cloning for EPC:** Using the techniques we have outlined in section 4, the EPC tag in an identity document may itself be authenticated by means of KBA or ABA. The authentication procedure itself would involve emission of the corresponding PIN, and therefore, to prevent eavesdropping attacks, might be best performed in a Faraday cage in cases where the border-control agent takes physical possession of cards. (KILL-based authentication also requires a precise physical layout to prevent tag destruction.)

2. **Improving privacy:** There are many opportunities to further improve the privacy properties of both the EDLs and the Passport Cards—and indeed many other uses of RFID tags. In addition to the standard cryptographic solutions, there are solutions that are backwards compatible with existing RFID reader deployments. For example, the EDLs and Passport Cards might incorporate capacitive sensors or gesture recognition techniques [12], and people might choose to use Blocker Tags instead of protective sheaths [24].

3. **Switch to another technology:** As an even stronger recommendation, we suggest that the DHS and other relevant entities consider adopting other technologies with stronger security and privacy properties. At one extreme, the relevant bodies might consider EDL- and Passport Card-equivalents that do not have embedded wireless technologies like RFIDs. At another extreme, the relevant bodies might consider the adoption of tamper-resistant RFID technologies with stronger cryptographic protection mechanisms.

6. CONCLUSION

In this paper, we have explored the issue of cloning in what could well become the most widely deployed radio device on the planet, the Class-1 Gen-2 EPC tag. As a point of departure and example, we have focused on deployment of these RFID tags in Passport Cards and Enhanced Drivers Licenses. We have shown that radio-layer cloning is a straightforward matter, but that the implications in the operational setting of border control are themselves somewhat more complicated.

The lessons we have gleaned here on cloning and anti-cloning extend well beyond the setting of EDLs and Passport Cards to EPC deployment in any setting where cloning or counterfeiting poses a risk. For example, with the encouragement of government regulators, the pharmaceutical industry is gradually embracing EPC for tracking and anti-counterfeiting at the prompting of the United States Food and Drug Administration [45], foreshadowing the technology's broad industry use as a security tool. Indeed, counterfeiting of consumer goods is a risk in nearly every industry. Thus the facts and ideas we have presented are of general interest in EPC deployment, particularly the read ranges of EPC tags and practical demonstration of the co-opting of EPC commands for anti-counterfeiting.

Acknowledgments

Our thanks to Garret Cole, Alexei Czeskis, Christina Drummond, Cynthia Matuszek, Kyle Rector, and Evan Welbourne.

7. REFERENCES

[1] L-1 identity solutions awarded the U.S. Passport Card program by the Department of State. *Business Wire*, 11 March 2008. Referenced 11 September 2008 at http://www.businesswire.com.

[2] New york to offer enhanced driver's license. *Newsday*, 16 September 2008. Referenced October 2008 at http://www.newsday.com/services/newspaper/printedition/tuesday/news/ny-nylice165845220sep16,0,5665783,print.story.

[3] Card format passport; changes to passport fee schedule [final action]; 22 cfr parts 22 and 51. *Federal Register*, 72(249):74169–74173, December 31, 2007. Referenced 2008 at http://www.gpoaccess.gov/fr.

[4] Card format passport; changes to passport fee schedule [proposed rule]; 22 cfr parts 22 and 51. *Federal Register*, 71(200):60928–60932, October 17, 2006. Referenced 2008 at http://www.gpoaccess.gov/fr.

[5] Smart Card Alliance. Comments of the smart card alliance to the department of state federal register notice,"card format passport; changes to passport fee schedule,ŠŠ 22 cfr parts 22 and 51, rin 1400-ac22, public notice 5558, 3 November 2006. Referenced 2008 at http://www.smartcardalliance.org/resources/pdf/Smart_Card_Alliance_Response_Passport_Card_Final.pdf.

[6] R. Anderson and M. Kuhn. Tamper resistance Ű a cautionary note. In *Second USENIX Workshop on Electronic Commerce*, pages 1–11, 1996.

[7] G. Avoine. Online bibliography: Security and privacy in RFID systems, 2008. Referenced 2008 at http://www.avoine.net/rfid.

[8] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security analysis of a cryptographically-enabled RFID device. In P. McDaniel, editor, *14th USENIX Security Symposium*, pages 1–16. USENIX, 2005.

[9] E. Borgida and R. E. Nisbett. The differential impact of abstract vs. concrete information on decisions. *Journal of Applied Social Psychology*, (7):258–271, 1977.

[10] S. Breznitz. *Cry Wolf: The Psychology of False Alarms*. Lawrence Erlbaum Associates, 1984.

[11] D. M. Caggiano and R. Parasuraman. The role of memory representation in the vigilance decrement. *Psychonomic Bulletin and Review*, 11(5):932–937, October 2004.

[12] A. Czeskis, K. Koscher, J. R. Smith, and T. Kohno. RFIDs and secret handshakes: Defending against ghost-and-leech attacks and unauthorized reads with context-aware communications. In *IEEE Symposium on Security and Privacy*, 2008.

[13] K. P. Fishkin, S. Roy, and B. Jiang. Some methods for privacy in RFID communication. In *1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, pages 42–53, 2004.

[14] R. Gerdes, T. Daniels, M. Mina, and S. Russell.

Device identification via analog signal fingerprinting: A matched filter approach. In *Network and Distributed System Security Symposium (NDSS)*, 2006.

[15] Marco Gruteser and Dirk Grunwald. A methodological assessment of location privacy risks in wireless hotspot networks. In *First International Conference on Security in Pervasive Computing*, pages 10–24, 2003.

[16] J. Halamka, A. Juels, A. Stubblefield, and J. Westhues. The security implications of VeriChip^{TM} cloning. *Journal of the American Medical Informatics Association (JAMIA)*, 13(5):601–607, November 2006.

[17] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. O'Hare. Vulnerabilities in first-generation RFID-enabled credit cards. In *Financial Cryptography*, pages 2–14, 2007.

[18] International Civil Aviation Organization ICAO. Document 9303, machine readable travel documents (MRTD), part I: Machine readable passports, 2005.

[19] EPCglobal Inc. Class 1 generation 2 UHF air interface protocol standard version 1.1.0. Referenced 2008 at http://www.epcglobalinc.org/standards/uhfc1g2/uhfc1g2_1_1_0-standard-20071017.pdf.

[20] M. Jakobsson and S. Wetzel. Security weaknesses in Bluetooth. In D. Naccache, editor, *The Cryptographer's Track at RSA*, volume 2020 of *Lecture Notes in Computer Science*, pages 176–191. Springer-Verlag, 2001.

[21] A. Juels. Strengthing EPC tags against cloning. In *ACM Workshop on Wireless Security (WiSe)*, pages 67–76. ACM Press, 2005.

[22] A. Juels. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communication*, 24(2), February 2006.

[23] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. In D. Gollman, G. Li, and G. Tsudik, editors, *SecureComm*, pages 74–88. IEEE, 2005. Referenced 2008 at http://eprint.iacr.org/2005/095.pdf.

[24] A. Juels, R.L. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In *8th ACM Conference on Computer and Communications Security*, pages 103–111. ACM Press, 2003.

[25] J. King and A. Mcdiarmid. Where's the beep?: security, privacy, and user misunderstandings of RFID. In *Useability, Psychology, and Security*, pages 1–8, 2008.

[26] R. S. Nickerson. Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, 2(2):175–220, 1998.

[27] K. Nohl, D. Evans, Starbug, and H. Plötz. Reverse-engineering a cryptographic RFID tag. In *USENIX Security*, 2008. To appear.

[28] F. Nylander. Alien Technology Higgs Gen2 IC LoadImage command application note 1 for 96 bit EPC memory, revision 7, 14 December 2006. Referenced 12 Sept. 2008 at http://www.alientechnology.com/docs/Load_Image_Applicaton_Note_1.pdf.

[29] M. C. O'Connor. Washington driver's licenses to carry EPC gen 2 inlays. *RFID Journal*, 30 July 2007. Referenced 2008 at http://www.rfidjournal.com/article/articleview/3514/1/1/.

[30] M. C. O'Connor. Industry group says e-passport clone poses little risk. *RFID Journal*, 9 August 2006. Referenced 2008 at http://www.rfidjournal.com/article/articleview/2559/1/1/.

[31] United States Department of Homeland Security. Privacy impact assessment for the use of radio frequency identification (RFID) technology for border crossings, 22 January 2008. Referenced 2008 at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_rfid.pdf.

[32] Washington State Department of Licensing. FAQ: EDL / ID, 2008. Referenced 2008 at www.dol.wa.gov/driverslicense/edlfaq.html.

[33] Washington State Department of Licensing. History of the EDL/ID program, 2008. Referenced 2008 at http://www.dol.wa.gov/driverslicense/edlhistory.html.

[34] OpenPCD project, 2008. Referenced 2008 at www.openpcd.org.

[35] M. R. Rieback, G. Gaydadjiev, B. Crispo, R. F. H. Hofman, and A. S. Tanenbaum. A platform for RFID security and privacy administration. In *USENIX LISA*, pages 89–102, 2006. Current project information referenced 2008 at www.rfidguardian.org.

[36] T. S. Saponas, J. Lester, C. Hartung, S. Agarwal, and T. Kohno. Devices that tell on you: Privacy trends in consumer ubiquitous computing. In *16th USENIX Security Symposium*, pages 55–70, 2007.

[37] B. Scheneier. The psychology of security, 18 January 2008. Referenced 2008 at http://www.schneier.com/essay-155.html.

[38] S.J. Sherman, K.S. Zehner, J. Johnson, and E.R. Hirt. Social explanation: The role of timing, set, and recall on subjective likelihood estimates. *Journal of Personality and Social Psychology*, 44:1127–1143, 1983.

[39] Read range for Gen2 RFID in 2008? 40 feet. *RFID Update*, 14 August 2008. Referenced 2008 at http://www.rfidupdate.com/articles/index.php?id=1656.

[40] L. J. Skitka, K. L. Mosier, and M. Burdick. Does automation bias decision-making? *Int. J. Human-Computer Studies*, 51:991–1006, 1999.

[41] J. R. Smith, A. P. Sample, P. S. Powledge, S. Roy, and A. Mamishev. A wirelessly-powered platform for sensing and computation. In *Ubicomp*, pages 495–506, 2006.

[42] C. Strohm. TSA to cut number of names on 'no-flyŠ list. *Government Executive*, 17 January 2007. Referenced 2008 at http://www.govexec.com/dailyfed/0107/011707tdpm1.htm.

[43] Identity Stronghold. Identity Stronghold's Secure Sleeve to protect US Passport Card. Company news release. Referenced 11 September 2008 at www.identitystronghold.com.

[44] Identity Stronghold. Washington State Enhanced Drivers License guarded by Identity Stronghold Secure Sleeve. Company annotation on news article. Referenced 11 September 2008 at www.identitystronghold.com/links.php.

[45] C. Swedberg. All eyes on FDA for drug e-pedigree. *RFID Journal*, 2008. Referenced 2008 at

http://www.rfidjournal.com/article/articleview/4013/1/1.
[46] Bureau of Consular Affairs United States Department of State. Western hemisphere travel initiative (whti) overview, 2008.
[47] N. D. Weinstein. Perceived probability, perceived severity, and health-protective behavior. *Health Psychology*, 19:65–74, 2000.
[48] J. Westhues. Hacking the prox card. In S. Garfinkel and B. Rosenberg, editors, *RFID: Applications, Security, and Privacy*, pages 291–300. Addison-Wesley, 2005.
[49] K. Witte and M. Allen. A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education and Behavior*, 27(5):591–615, 2000.

APPENDIX

A. ANTENNA IMAGES

Since the Washington State Enhanced Drivers License and Passport Card have different performance characteristics, we investigated the antenna configuration inside each card. We backlit both cards in a dark room and photographed them up close. We blurred out certain personally-identifiable information the cardholders do not want public. These images are shown in figures 2 and 3.

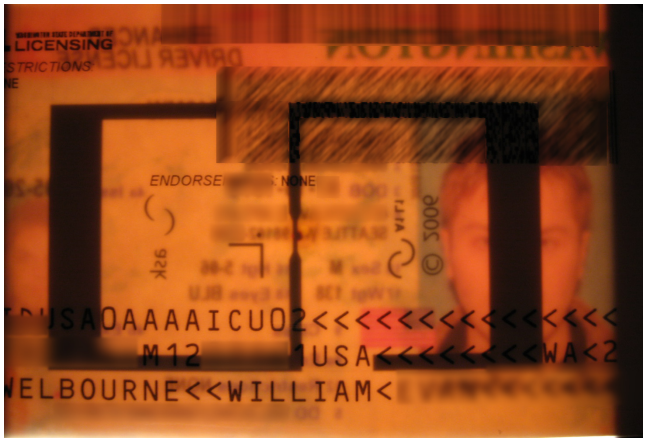


Figure 2: The antenna inside a Washington State Enhanced Drivers License. Certain personally-identifiable information has been obscured.

Figure 3: The antenna inside a Passport Card. Certain personally-identifiable information has been obscured.

B. EXPERIMENTAL RESULTS FOR SCALED KBA

Here we report experimental results on our scaled KBA technique omitted from the main body of the paper. In Table 6, we report reader power measurements. For 100 iterations of scaled KBA, we list the mean minimum read and write power levels found, as well as their standard deviations. In Table 7, we report timing results. The mean time to determine the minimum read and write power levels, and to perform the write and authentication tests, are reported.

B.1 Received Signal Strength Indicator (RSSI) Measurements - Rx

Gen 2 RFID framework is implemented using UHF (Ultra High Frequency) spectrum, make it suitable for uses where high data rates and longer distance are needed. However UHF suffers form one major drawback and that is that signals do not pass easily through materials as it is the case with RFIDs which work on lower frequencies. *Dense reader environment* amplifies this effect even to greater extent, even though Gen 2 implements *Dense Reader Mode Protocol* which tries to eliminate reading interferences. Furthermore RSSI varies based on the CW (continuous wave) configuration or modulation technique utilized by the manufacturer. Additionally, objects to which the tag is mounted and the orientation of the tag to the reader depending on antenna configurations will dramatically impact the RSSI output. Even the binary representation of a tags ID number as it is modulated for RF can show a variance in RSSI from one tag to another situated right next to each other. Fortunately, several of issues addressed about have a symmetric property and some of them can be easily discarded as problematic. Symmetry implies that the issue is bidirectional, from tag to reader and vice versa.

The experiment we conducted was done in a very noisy environment, consisted of multiple readers interfering with each each other giving very inconsistent readings (Figure 1). Setup was fairly simple. We had a single tag that was being probed in clear line of sight. Our first goal was to determine if there was any meaning that could be extracted from these erratic readings. Given the setup above, we took n number of readings and recorded those values. Afterward we kept on shifting the tag few centimeters at a time and recording those values as well. The results were as following. Taking the average of values for each of the measurements reveled interesting results. We were able to effectively determine relative distance based on the averaged RSSI readings.

B.2 Power Calibration - Tx

Based on the received RSSI values, we need to be able to produce a kill commands in a way that would result in *Insufficient Power* response. The first task was to see how fast the power setting could be calibrated.

B.2.1 Measuring Power Calibration Time Interval

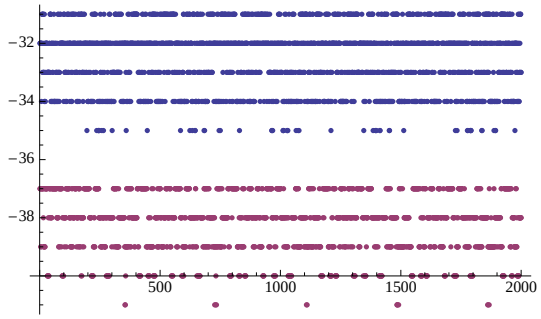
After we acquired the values for time interval required for reader to calibrate its power, we took the average which was around $0.07s$.

Distance	Mean Min. Read Power	SD Min. Read Power	Mean Min. Write Power	SD Min. Write Power
10 cm	15.3	0	15.0	0.0
20cm	15.3	0	15.0	0.2
30cm	15.3	0	15	0
40cm	15.3	0	15	0
50cm	15.3	0	15.1	0.1
60cm	15.3	0.1	17.1	0.2
70cm	15.7	0.9	17.7	0.8
80cm	15.3	0.4	17.6	0.4
90cm	15.6	0.4	17.9	0.4
100cm	17.7	0.9	20.1	0.8
110cm	18.0	0.9	20.3	0.9
120cm	21.2	1.3	22.9	1.3
130cm	20.4	1.3	22.8	1.2
140cm	22.3	1.6	24.7	1.5
150cm	19.8	0.8	22.5	0.8
160cm	20.0	1.0	22.4	0.8
170cm	19.6	0.8	22.4	0.7
180cm	21.8	0.5	24.8	0.5
190cm	18.7	0.6	21.4	0.6
200cm	21.6	0.8	24.6	1.1

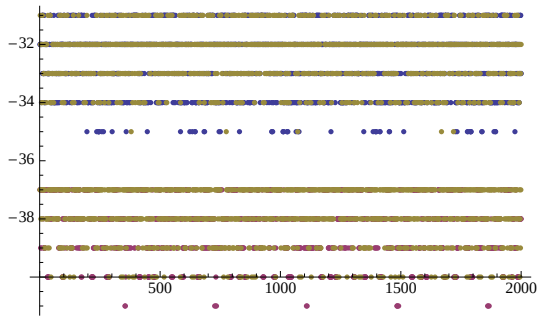
Table 6: Scaled KBA Power calibration results (All measurements are in dBm)

Distance	Mean Read Calib. Time	Mean Write Calib. Time	Mean Write Test Time	Mean PIN Test Time	
10cm	374 ms	73.0 ms	N/A	N/A	
20cm	384 ms	75.7 ms	N/A	N/A	
30cm	352 ms	70.9 ms	N/A	N/A	
40cm	383 ms	74.8 ms	N/A	N/A	
50cm	376 ms	84.8 ms	N/A	N/A	
60cm	392 ms	343 ms	334 ms	44.7 ms	
70cm	422 ms	361 ms	435 ms	54.1 ms	
80cm	411 ms	383 ms	352 ms	45.1 ms	
90cm	435 ms	395 ms	453 ms	50.7 ms	
100cm	403 ms	408 ms	636 ms	73.7 ms	
110cm	399 ms	355 ms	594 ms	77.7 ms	
120cm	378 ms	314 ms	580 ms	67.7 ms	
130cm	401 ms	409 ms	586 ms	51.3 ms	
140cm	385 ms	304 ms	576 ms	63.4 ms	
150cm	389 ms	420 ms	542 ms	87.8 ms	
160cm	396 ms	422 ms	532 ms	53.3 ms	
170cm	388 ms	455 ms	523 ms	57.2 ms	
180cm	373 ms	461 ms	540 ms	49.8 ms	
190cm	378 ms	396 ms	469 ms	52.8 ms	
200cm	379 ms	413 ms	547 ms	53.2 ms	

Table 7: Scaled Timing and Reliability Results



(a) Independent Readings



(b) Power Switching

Figure 4: `Blue` - 32dB, `Red` - 16dB, `Yellow` - Switched

Even though, the measurements were very consistent, with low standard deviation gave us little insight in if the power calibration was actually finished within the hardware. In order to verify this, we had to come up with a new scheme. The only difference in the pseudo code from the above is that the power level would alternate from low to high power setting and whenever the power setting was altered we read exactly one RFID tag and recorded its RSSI value. In other words, making two different measurements with opposite power levels with no overlapping values should not differentiate from scheme above where we keep on alternating the power level. Here is the graph representing the results.

Surprisingly, hardware and software calibration happen at the same time as it can be seen from Figure 4. If it were not the case that the power calibration was done completely, we would have seen some values floating between low and high power level regime.

B.3 Insufficient Power Protocol

Establishing the fact that the power calibration does adhere to the given specification, our next major task was to design a protocol that would allow us to send a kill command and in return get a *Not Enough Power* response. Due to noisy testing environment, a protocol had to be designed in such a way that probing a tag would not result in an accidental kill. In order to achieve this, a statistical analysis would need to be done - specifically, given a wanted CI (Confidence Interval) we need to determine how many packets at some signal strength level would need to be sent in order to satisfy given CI.

It is important to notice that there is one to one correlation between $RSSI_{TX}$ and $RSSI_{RX}$ - i. e. strength of signal transmitted to get *Not Enough Power Response* and the received signal strength of that same RFID. This allows us to *eliminate* ranges for which we are certain we will not get any response whatsoever, increasing the speed of the overall process. After collecting the data, we create *lookup table* which we will use to set the initial power settings to, determined by the power level we receive from the RFID. The lookup table has to be done manually, and it differs from one RFID/Reader implementation to another.

In conclusion, the protocol does work with small error associated with it. The reason why it fails in some small subset of tries is unknown and hard to determine only using software.